InCharge Systems, Inc.
1128 20th Street, West Des Moines, IA 50265

VIA ECFS

April 13, 2011

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W., Room TW-A325
Washington, D.C. 20554.

Re: Comments on *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*.
WC Docket No. 11-39. FCC 11-41.

Dear Ms. Dortch:

I appreciate the opportunity to represent InCharge Systems, Inc. (ICS) by sharing the following comments related to the Federal Communications Commission (FCC) Notice of Proposed Rulemaking (NPRM) in the matter of Rules and Regulations Implementing the Truth in Caller ID Act of 2009 WC Docket No. 11-39, FCC 11-41. ICS is a development stage company whose primary focus since inception has been on IP communications security solutions. Within this context, the company has built up a deep understanding of the issues around security, identity and authentication. Our comments relate to the ease of caller ID spoofing and an existing solution for detecting manipulated caller ID information, along with some issues about benefits and barriers.

Caller ID spoofing attacks have become easier.

While the problem of Caller ID spoofing manifests itself in various specific attacks, including but not limited to examples referenced in Section I of the NPRM, the common underlying source of such attacks is the *ease* with which bad actors are able to engage in spoofing. The growing deployment of VoIP is a primary cause of that ease, both because the underlying IP network is open, making the attackers difficult to detect, and because the tools of the attackers' trade are readily available, inexpensive, and require minimal expertise to implement/operate.

When the Commission first adopted rules relating to calling party number (CPN), Common Carriers that utilized SS7 signaling for call set-up were able to deploy a network-based approach that allowed a caller's number to be displayed at the dialed number's terminal or at any called service desk (e.g. E911) by reading the calling number from the Initial Address Message (IAM) encapsulated into the call set-up signal by the originating caller's local calling office. While it was technically feasible to attack Caller ID services delivered in such a manner over SS7 networks, the coupling of the application as part of the transport network rendered such attacks highly challenging for most users. As a result, Caller ID services were highly reliable in this closed network and were trusted by recipients.

Today, in order to avoid detection, bad actors exploit the decoupling of IP network connectivity from the voice application, while knowingly engaging in caller ID spoofing by downloading free software that allows them the ability to assert a Caller ID of the originator's choice. The consequence of such spoofing is that recipients can no longer trust caller ID services.

Manipulated caller ID information can be detected.

As a result of the ease of spoofing, rules that rely on legislative prohibitions and resulting penalties for violation should be expected to be obeyed by legitimate users, but largely ignored by the bad actors toward whom the legislation is directed, which limits the impact and benefits of the current proposed rules.

However, there is an existing standards-based technological solution with significant *preventative* benefits that the FCC could communicate back to Congress via the mandated Report as described in NPRM paragraph's 10 and 35. The FCC could request additional authority to adopt rules requiring originators of interconnected VoIP calls to assign a cryptographic signature as part of the originating call request.

These digital signatures can authenticate an originator's caller ID information, and can be validated anywhere along the call path, including by the recipient of the call, as well as by transport or terminating network providers. This would provide a solution that enables relying parties to know if the received caller ID information has been manipulated (see the NPRM paragraph 13).

The Internet Engineering Task Force (IETF) has also recognized the spoofing problem in interconnected VoIP services that Congress is seeking to prevent. As a result, the IETF adopted RFC 4474 ("Enhancements for Authenticated Identity Management in SIP"), which describes a solution to the problem of caller ID spoofing. RFC 4474 describes a method relying on PKI (public key infrastructure) techniques to digitally sign the set-up of such calls, allowing relying parties to authenticate the validity of the originators Caller ID through a neutral third-party certificate authority. The Introduction section of RFC 4474 states: "... in the telephone network today [referencing the SS7 network], one can receive a call from someone with whom one has no previous association, and still have a reasonable assurance that the person's displayed Caller-ID is accurate. A cryptographic approach, like the one described in this document, can probably provide a much stronger and less-spoofable assurance of identity than the telephone network provides today." Figure 1 below depicts a basic implementation.

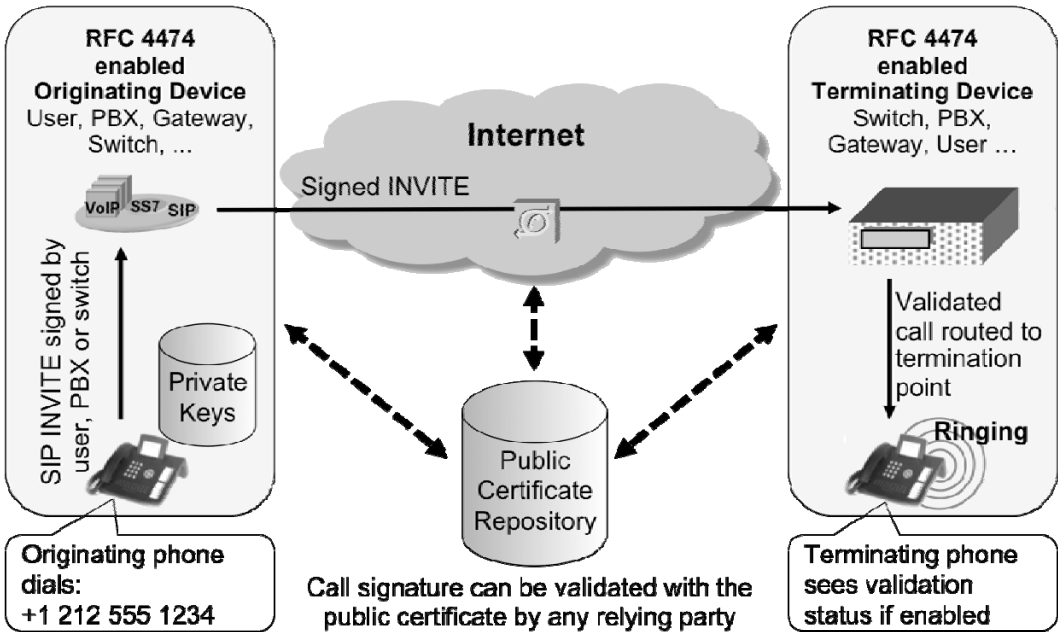

Figure 1

There are benefits and barriers related to technical solutions.

There are benefits to a solution using digital signing and validation to combat spoofing. Using key pairs and certificates associated with telephone numbers and caller ID information is based on proven cryptographic technology. This approach supports authentication and detection anywhere along the call path. It separates the issue of whether a user is authorized to use a phone number from the mechanics of adding security features during call setup.

In particular cases, this solution can readily identify incoming calls that include signed and validated Caller IDs. For example, E911 PSAPs (public safety answering points) could use such an approach: valid calls could be accepted, while incoming calls that are unsigned or that fail validation could be dealt with according to anti-spoofing policies (see NPRM paragraph 17).

In another instance, this solution could be applied to caller ID spoofing services when used for the legitimate maintenance of privacy or anonymity as mentioned in the NPRM. If signed call setup requests were used, then the operations of caller ID spoofing services could add a degree of trust for their calls. Public authorities could use policies for the handout and storage of translation requests to facilitate a non-repudiation service for trusted Caller ID spoofing services. In addition to information management, policies could include automatic handling for valid signed requests or/and operator assisted handling for unsigned or invalid signed requests.

In general, it is envisioned that this solution, could lead to a much lower proportion of possibly spoofed calls in many areas, and this knowledge should benefit any intermediate party or call recipient. In brief, policy-based handling of incoming calls is enhanced by knowing the result of validating them.

However, there are always barriers to change. In this situation, the burdens seem shifted towards the calling party or originating provider, while the benefits seem to apply more towards the relying parties - call recipients, transport and/or terminating providers. It seems likely that legislation and/or regulation would be useful for helping to incentivize signing and validation to combat caller ID spoofing.

Conclusion

In conclusion, spoofing of Caller ID is a serious problem today that is certain to grow in frequency and severity, consistent with the ongoing deployment of successor VoIP technologies, which facilitate attack vectors utilized by bad actors. Due to the wide availability of attack tools, coupled with the ease with which attackers are able to maintain anonymity, it should be expected that regulations designed to be preventative will need to go beyond reactive prohibitions in order to achieve the desirable intended results.

By utilizing the required Report to Congress to request the authority to implement preventive regulations, i.e., requiring that originators of interconnected VoIP calls employ existing standards to assign a cryptographic signature to the call set-up at the time the call is originated, the Commission could facilitate significant mitigation of the attacks from which Congress seeks to provide protection. We would welcome an opportunity for some additional discussion of the suggestions provided above.

Respectfully submitted,

/s/ Warren Bent

Warren Bent, Vice President, Business Development
InCharge Systems, Inc.
724 Duane Street
Glen Ellyn, IL. 60137
warrenbent@inchargesys.com
+1.630.474.9451